

M303 Pure Mathematics
2015 Exam M303/J
Unofficial Solutions
(Version 14)

Collaboration by Contributors to M303 Forum discussions
'Answers from You All', '2015 Exam - Draft Student Solutions'

Jonathan Anderson, Ross Creed, Anthony Keenan,
David Knowles, David Morgan, Carmel O'Reilly, Robert Shaw,
Lisa Smith, Andy Summerskill, Fulvio Tabacco,
Peter Winter-Smith
etc etc

2019
Cristiano Broccias, Bob Senior

2020
Andrew Belton

5th May 2021

Question 1

- (a) For $n = 2$ we have $10^n - 4 = 10^2 - 4 = 96 = 12 \times 8$, which is divisible by 12. This gives a basis for the induction.

Assume that the statement “ $10^n - 4$ is divisible by 12” is true for $n = k$. Then:

$$\begin{aligned} 10^{k+1} - 4 &= 10(10^k) - 4 \\ &= 10(10^k) - 40 + 36 \\ &= 10(10^k - 4) + 36 \end{aligned}$$

Since $10^k - 4$ is divisible by 12 (by the induction hypothesis) and 36 is divisible by 12, $10^{k+1} - 4$ is divisible by 12.

So the hypothesis is true for $n = 2$, and if $n = k$ is true then $n = k + 1$ is true, so by the Principle of Mathematical Induction (generalised), HB, page 14 the hypothesis is true for all integers $n \geq 2$.

(b)

- (i) If $a \equiv b \pmod{n}$ then we can find an integer p such that:

$$\begin{aligned} a - b &= pn \\ ka - kb &= kpn \\ ka - kb + c - c &= kpn \\ (ka + c) - (kb + c) &= (kp)n \end{aligned}$$

Which, from the definition of congruence implies that $ka + c \equiv kb + c \pmod{n}$.

- (ii) If $ka \equiv b \pmod{n}$ and $kc \equiv d \pmod{n}$ then we can find integers p and r such that:

$$\begin{aligned} ka - b &= pn \\ kac - bc &= cpn \end{aligned} \tag{1.1}$$

Similarly:

$$\begin{aligned} kc - d &= rn \\ kac - ad &= arn \end{aligned} \tag{1.2}$$

Subtracting (1.2) from (1.1)

$$\begin{aligned} kac - bc - (kac - ad) &= cpn - arn \\ kac - kac + ad - bc &= (cp - ar)n \\ ad - bc &= (cp - ar)n \end{aligned}$$

So $ad \equiv bc \pmod{n}$ as required.

- (iii) If $ra \equiv rb \pmod{rn}$ then we can find an integer p such that:

$$\begin{aligned}ra - rb &= prn \\a - b &= pn\end{aligned}$$

So if $ra \equiv rb \pmod{rn}$ then $a \equiv b \pmod{n}$.

Similarly, if $a \equiv b \pmod{n}$ we can find an integer q such that:

$$\begin{aligned}a - b &= qn \\ra - rb &= rqn\end{aligned}$$

So if $a \equiv b \pmod{n}$ then $ra \equiv rb \pmod{rn}$. It follows that $ra \equiv rb \pmod{rn}$ if, and only if, $a \equiv b \pmod{n}$.

- (c) As $n \equiv 3 \pmod{8}$ we have $n = 8k + 3$, giving $5n + 3 = 5(8k + 3) + 3 = 40k + 18$.
- (i) Since $4|40$ and $18 \equiv 2 \pmod{4}$ we have $5n + 3 \equiv 2 \pmod{4}$
- (ii) Since $20|40$ and $18 \equiv 18 \pmod{20}$ we have $5n + 3 \equiv 18 \pmod{20}$

Question 2

(a)

(i) $\mathbb{Z}_{12}, \mathbb{Z}_9$ are trivially cyclic.

Now for the other groups to be determined you use Proposition 2.10 of the HB p 32, which states:

“The direct product $\mathbb{Z}_m \times \mathbb{Z}_n$ of the cyclic groups $\mathbb{Z}_m$ and $\mathbb{Z}_n$ is cyclic if, and only if, m and n are coprime positive integers.”

and so $\text{hcf}(6, 2) = 2$ and so $\mathbb{Z}_6 \times \mathbb{Z}_2$ is not cyclic; $\text{hcf}(4, 3) = 1$ so $\mathbb{Z}_4 \times \mathbb{Z}_3$ is cyclic. Further $\text{hcf}(3, 3) = 3$ so $\mathbb{Z}_3 \times \mathbb{Z}_3$ is not cyclic.

Now $\text{hcf}(3, 2) = 1$ and so by Corollary 2.12 HB page 32, $\mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6$, hence $\mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6 \implies \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_6 \times \mathbb{Z}_2$. However $\text{hcf}(6, 2) = 2$ and so $\mathbb{Z}_6 \times \mathbb{Z}_2 \not\cong \mathbb{Z}_{12}$

Hence the cyclic groups in the list are $\mathbb{Z}_{12}, \mathbb{Z}_9$, and $\mathbb{Z}_4 \times \mathbb{Z}_3$

(ii) $|\mathbb{Z}_9| = |\mathbb{Z}_3 \times \mathbb{Z}_3| = 9$ and $6 \nmid 9$ and by Proposition 4.5 p29 of the HB the order of an element in a group has to divide the order of the group and so neither $\mathbb{Z}_9$ or $\mathbb{Z}_3 \times \mathbb{Z}_3$ can have an element of order 6.

- $2 \in \mathbb{Z}_{12}$ has order 6.
- $(1, 0) \in \mathbb{Z}_6 \times \mathbb{Z}_2$ has order 6.
- $(2, 1) \in \mathbb{Z}_4 \times \mathbb{Z}_3$ has order 6.
- $(1, 1, 0) \in \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has order 6.

and so the only groups in the list that do not have an element of order 6 are $\{\mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3\}$

(iii) I have already shown that $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_6 \times \mathbb{Z}_2$ in Q2(a)(i).

Using Corollary 2.12 HB page 32 and using the fact that $\text{hcf}(4, 3) = 1$, I conclude that $\mathbb{Z}_4 \times \mathbb{Z}_3 \cong \mathbb{Z}_{12}$.

Also as $\text{hcf}(3, 3) = 3$ I deduce from Corollary 2.12 that $\mathbb{Z}_3 \times \mathbb{Z}_3 \not\cong \mathbb{Z}_9$.

Hence the only pairs that are isomorphic are $\mathbb{Z}_4 \times \mathbb{Z}_3 \cong \mathbb{Z}_{12}$ and $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_6 \times \mathbb{Z}_2$.

(b) We are given in the presentation of the group that $aba^3b = e$ also we are given that $a^4 = e$ so that means $a^4 = a^3a = e \implies a^{-1} = a^3$ and so

$$\begin{aligned} aba^3b = e &\implies \\ aba^{-1}b = e &\implies \\ aba^{-1} = b^{-1} &\implies \\ ab = b^{-1}a &\implies \\ bab = a & \end{aligned}$$

and so $bab = a$

- (c) We use Sylow's theorems to show that the group, G say, of order 54 only has one Sylow 3-subgroup and then by Lemma 1.9 page 39 of the Handbook that Sylow 3-subgroup would be normal and hence G would contain a non-trivial proper normal subgroup and hence not be simple.

As $54 = 2 \times 3^3$ by Sylow's First Theorem HB page 39 the number of Sylow 3-subgroups is at least 1. Now the number of Sylow 3-subgroups has to satisfy $m \equiv 1 \pmod{3}$ by Sylow's Second Theorem and hence $m \in \{1, 4, 7, \dots\}$. However combining this fact with Sylow's Third Theorem (b) HB page 39, means that m has to divide 2 and so $m = 1$ and the result follows from the previous discussion.

Question 3

(a)

- (i) Although the introductory passage tells you
- σ
- is multiplicative this is a bit of a red herring.

Given

 $\sigma(p) = p + 1$ and $2n + \sigma(n) \equiv 0 \pmod{3}$ and n is prime (so can use $p = n$) then:

$$2n + (n + 1) \equiv 0 \pmod{3}$$

$$3n + 1 \equiv 0 \pmod{3}$$

$$1 \equiv 0 \pmod{3}$$

This is a contradiction so one of the assumptions must be false.

The first two are given, so it must be the assumption that n was prime.It follows that if $2n + \sigma(n) \equiv 0 \pmod{3}$ (for the definition of sigma) then n is not prime

(ii)

From our handbook $\sigma(p^2) = p^2 + p + 1$ so if $n = p^2$:

$$2n + \sigma(n) \equiv 0 \pmod{3}$$

$$2p^2 + \sigma(p^2) \equiv 0 \pmod{3}$$

$$2p^2 + p^2 + p + 1 \equiv 0 \pmod{3}$$

$$3p^2 + p + 1 \equiv 0 \pmod{3}$$

$$p \equiv -1 \equiv 2 \pmod{3} \text{ as required.}$$

- (iii) Again
- $\sigma(p^3) = p^3 + p^2 + p + 1$
- so if
- $n = p^3$
- :

$$2n + \sigma(n) \equiv 0 \pmod{3}$$

$$2p^3 + \sigma(p^3) \equiv 0 \pmod{3}$$

$$2p^3 + p^3 + p^2 + p + 1 \equiv 0 \pmod{3}$$

$$p^2 + p \equiv 2 \pmod{3}$$

Clearly $p \neq 0$ and $p \neq 2$ so $p \equiv 1 \pmod{3}$ and hence $p \equiv 1 \pmod{6}$ or $p \equiv 4 \pmod{6}$.If $p \equiv 4 \pmod{6}$ then p is not prime so $p \equiv 1 \pmod{6}$, as required.

- (b) Let
- $f(x) = 8x^3 - 6x - 1$
- . Then
- f
- is a polynomial in the ring of integers
- $\mathbb{Z}[x]$
- and 7 is a prime that does not divide the leading coefficient 8. By Lemma 4.19 HB p51, it is sufficient to show that
- f
- is irreducible in the ring of integers subscript
- $\mathbb{Z}_7[x]$
- . We shall verify that no element
- $a \in \mathbb{Z}_7[x]$
- is a root of
- f
- .

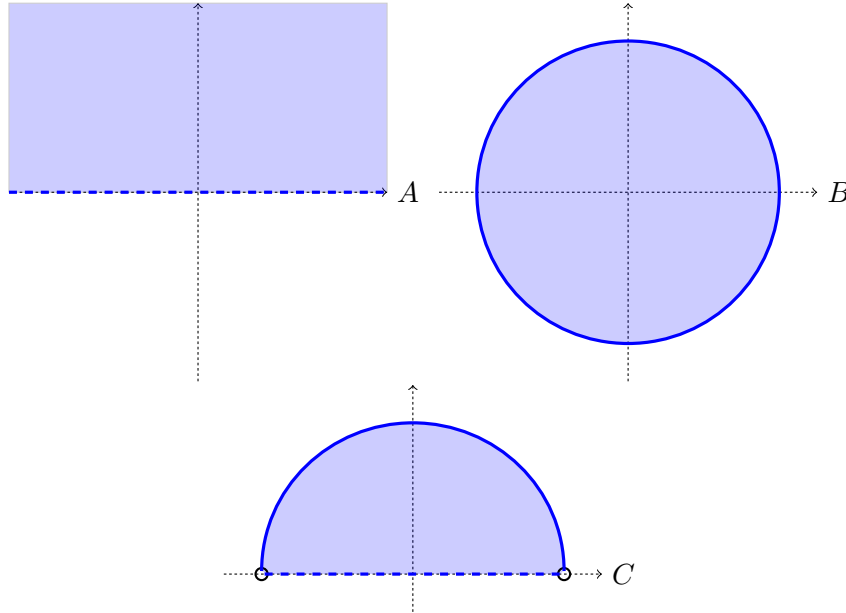
Testing each of these elements:

$$\begin{aligned}0^3 + 0 - 1 &\equiv -1 \\1^3 + 1 - 1 &\equiv 1 \\2^3 + 2 - 1 &\equiv 2 \\3^3 + 3 - 1 &\equiv 1 \\-3^3 - 3 - 1 &\equiv -3 \\-2^3 - 2 - 1 &\equiv -4 \\-1^3 - 1 - 1 &\equiv -3 \pmod{7}\end{aligned}$$

Thus by Lemma 4.19, $8x^3 - 6x - 1$ is irreducible over the ring $\mathbb{Z}$.

Question 4

(a)



(b)

(i)

$$\begin{aligned}
 \text{Cl}_{(\mathbb{R}^2, d^{(2)})}(C) &= \{(a, b) \in \mathbb{R}^2 : a^2 + b^2 \leq 4, b \geq 0\}, \\
 \text{Int}_{(\mathbb{R}^2, d^{(2)})}(C) &= \{(a, b) \in \mathbb{R}^2 : a^2 + b^2 < 4, b > 0\}, \\
 \text{Bd}_{(\mathbb{R}^2, d^{(2)})}(C) &= \text{Cl}_{(\mathbb{R}^2, d^{(2)})}(C) - \text{Int}_{(\mathbb{R}^2, d^{(2)})}(C) \\
 &= \{(a, b) \in \mathbb{R}^2 : a^2 + b^2 = 4, b > 0\} \cup \{(a, 0) \in \mathbb{R}^2 : -2 \leq a \leq 2\}
 \end{aligned}$$

(ii)

$$\begin{aligned}
 \text{Cl}_{(\mathbb{R}^2, e)}(C) &= \{(a, b) \in \mathbb{R}^2 : a^2 + b^2 \leq 4, b > 0\} \\
 \text{Int}_{(\mathbb{R}^2, e)}(C) &= \{(a, b) \in \mathbb{R}^2 : a^2 + b^2 < 4, b > 0\} \\
 \text{Bd}_{(\mathbb{R}^2, e)}(C) &= \text{Cl}_{(\mathbb{R}^2, e)}(C) - \text{Int}_{(\mathbb{R}^2, e)}(C) = \{(a, b) \in \mathbb{R}^2 : a^2 + b^2 = 4, b > 0\}
 \end{aligned}$$

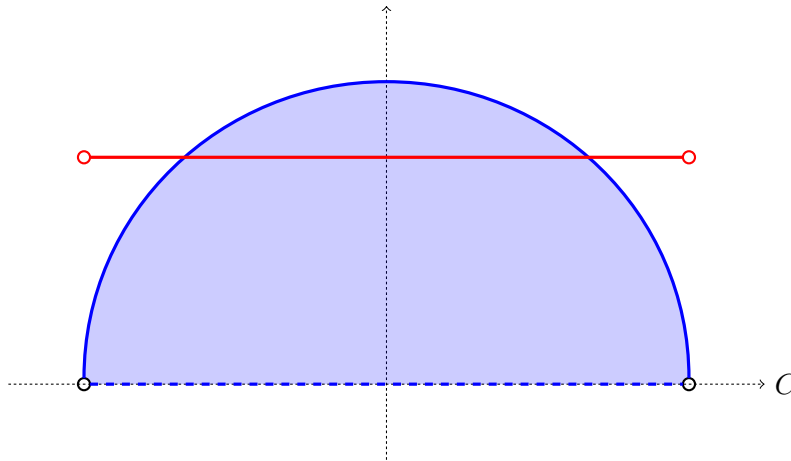
(c) **Method 1**

Let $\mathcal{S} = \{U_b : 0 < b \leq 2\}$ where $U_b = \{(x, b) : -2 < x < 2\}$

Then $\mathcal{S}$ is an open cover of C for which there is no finite subcover.

A typical member of $\mathcal{S}$ is shown below,

In discussions, three different approaches to part (c) emerged and there is merit in including all three.



Method 2

Consider the sequence $(\mathbf{x}_n)_{n \in \mathbb{N}} \subseteq C$ where $\mathbf{x}_n = \left(0, \frac{1}{n}\right)$ and suppose that it contains a convergent subsequence $\mathbf{x}_{n_i} \xrightarrow{e} \mathbf{x}$, where $\mathbf{x} = (a, b) \in C$. Then, by definition, $e(\mathbf{x}_{n_i}, \mathbf{x})$ is a null sequence, i.e.

$$e(\mathbf{x}_{n_i}, \mathbf{x}) = |0 - a| + d_0\left(\frac{1}{n_i}, b\right) \rightarrow 0$$

as $n \rightarrow \infty$.

By inspection, this implies $a = 0$, so $\mathbf{a} = (0, b)$ and

$$e(\mathbf{x}_{n_i}, \mathbf{x}) = d_0\left(\frac{1}{n_i}, b\right)$$

should be a null sequence.

But by definition of discrete metric, this is possible only if $(\mathbf{x}_n)_{n \in \mathbb{N}}$ contained an eventually constant sequence, which it does not because all its terms are different, so our suppositions leads to a contradiction.

Therefore $(\mathbf{x}_n)_{n \in \mathbb{N}}$ is a sequence in C that does not contain a convergent subsequence, so C is not sequentially compact, hence it is not compact by Theorem 5.10, page 133, HB.

Method 3

I start by showing that C is not totally bounded then Corollary 5.7 and Lemma 5.2 page 133 of the HB implies that C is not sequentially compact. As then C is not sequentially compact Theorem 5.12 page 134 of the HB implies that C is not compact.

Now the definition of totally bounded (Definiton 5.5 page 133 of HB) is as follows “A metric space (C, e) is totally bounded if there is a finite ε -net for each $\varepsilon > 0$ ” and so I now show that for $\varepsilon = \frac{1}{2}$ no such finite ε -net exists.

Working from the definition of a ε -net page 132 of the HB I have to show that,

$$C \not\subseteq \bigcup_{p \in N(\frac{1}{2})} B_e(p, \frac{1}{2})$$

However $\{(0, a) \in \mathbb{R}^2: 0 < a < 2\} \subset C$ and so it's sufficient to show,

$$\{(0, a) \in \mathbb{R}^2: 0 < a < 2\} \not\subset \bigcup_{p \in N(\frac{1}{2})} B_e(p, \frac{1}{2})$$

Now as $B_e(p, \frac{1}{2})$ for sum $p \in N(\frac{1}{2})$ is a horizontal line of at most length one unit and $\{(0, a) \in \mathbb{R}^2: 0 < a < 2\}$ is a vertical line of length 2 units then $B_e(p, \frac{1}{2}) \cap \{(0, a) \in \mathbb{R}^2: 0 < a < 2\}$ can at most contain one point in C and as $N(\frac{1}{2})$ contains only a finite amount of points, n say, in C this implies that $\bigcup_{p \in N(\frac{1}{2})} B_e(p, \frac{1}{2})$ can at most only contain n points in $\{(0, a) \in \mathbb{R}^2: 0 < a < 2\}$. However $\{(0, a) \in \mathbb{R}^2: 0 < a < 2\}$ contains an infinite number of points and so this implies,

$$\{(0, a) \in \mathbb{R}^2: 0 < a < 2\} \not\subset \bigcup_{p \in N(\frac{1}{2})} B_e(p, \frac{1}{2})$$

and hence C is not totally bounded and so not sequentially compact and so not compact.

Question 5

- (a) We have $J = \langle 5, 3 - i \rangle$. $\mathbb{Z}[i]$ is a PID and so $J = \langle z \rangle$ where $z = \text{hcf}(5, 3 - i)$.

Lemma 3.7 HB
p97

Since $N(5) = 5^2 = 25$ and $N(3 - i) = 3^2 + 1^2 = 10$, we divide $3 - i$ into 5.

Using the Euclidean Algorithm,

$$\frac{5}{3 - i} = \frac{5(3 + i)}{(3 - i)(3 + i)} = \frac{15 + 5i}{10} = \frac{3}{2} + \frac{1}{2}i.$$

Taking the nearest Gaussian integer 1,

$$5 = (3 - i) + \left(\frac{1}{2} + \frac{1}{2}i\right)(3 - i) = (3 - i) + (2 + i).$$

Alternatively, we may just observe that $5 = (3 - i) + (2 + i)$.

Taking a further step,

$$\frac{3 - i}{2 + i} = \frac{(3 - i)(2 - i)}{(2 + i)(2 - i)} = \frac{5 - 5i}{5} = (1 - i) + 0,$$

and so $\text{hcf}(5, 3 - i) = 2 + i$, up to associates.

The units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$ and so $J = \langle z \rangle$ when

$$z = 2 + i, -2 - i, -1 + 2i \text{ and } 1 - 2i.$$

- (b) For any of the values of z , if $z = ab$ then $N(a)N(b) = N(z) = 5$.

Norm is
multiplicative

But 5 is a prime in $\mathbb{Z}$ and has no proper factors, so $N(a)$ or $N(b)$ equals 1.

Thus one of a or b is a unit, and so z is irreducible.

Defn 2.5 HB p53

Since $\mathbb{Z}[i]$ is a PID and z is irreducible, $J = \langle z \rangle$ is a maximal ideal.

Th. 4.22 HB p99

Since J is a maximal ideal, $\mathbb{Z}[i]/J$ is a field.

Th. 4.23 HB p99

Question 6

- (a) To show that A is $d_{\max}$ -sequentially compact, Theorem 3.12 HB pg 131 tells us to prove that:

1. A is $d_{\max}$ closed,
2. A is a pointwise bounded set of functions,
3. A is an equicontinuous set of functions.

Hypothesis 1:

Let (f_n) be a sequence of functions in A that converges to $f \in C[0, 1]$ for $d_{\max}$.

We need to show that $f \in A$.

Since $|f_n(x)| \leq x^2$ for each $n \in \mathbb{N}, x \in [0, 1]$, we have,

$$\begin{aligned} |f(x)| &= |f(x) - f_n(x) + f_n(x)| \\ &\leq |f(x) - f_n(x)| + |f_n(x)| \\ &\leq d_{\max}(f_n, f) + x^2 \end{aligned}$$

But $d_{\max}(f_n, f)$ is a null sequence and so $|f(x)| \leq x^2$ for each $x \in [0, 1]$.

For $x, y \in [0, 1]$ we can use the Triangle Inequality (for modulus) and the fact that $f_n \in A$ implies that for each $n \in \mathbb{N}$,

$$\begin{aligned} |f(x) - f(y)| &\leq |f(x) - f_n(x)| + |f_n(x) - f_n(y)| + |f_n(y) - f(y)| \\ &\leq d_{\max}(f_n, f) + |f_n(x) - f_n(y)| + d_{\max}(f_n, f) \\ &\leq 2d_{\max}(f_n, f) + |f_n(x) - f_n(y)| \\ &\leq 2d_{\max}(f_n, f) + 2\sqrt{|x - y|} \end{aligned}$$

But $d_{\max}(f_n, f)$ is a null sequence and so $|f(x) - f(y)| \leq 2\sqrt{|x - y|}$ for $x, y \in [0, 1]$.

Hence $f \in A$ and so A is $d_{\max}$ closed.

Hypothesis 2: Let $x \in [0, 1]$. Then for each $f \in A$,

$$|f(x)| \leq x^2$$

This bound does not depend on the choice of f , so A is a pointwise bounded family of functions.

Hypothesis 3:

Let $\varepsilon > 0$. If $x, y \in [0, 1]$ and $|x - y| < \delta$, then for each $f \in A$,

$$|f(x) - f(y)| \leq 2\sqrt{|x - y|} < 2\sqrt{\delta}$$

In particular, if $\delta = \varepsilon^2/4$,

then

$$2\sqrt{|x-y|} \leq 2\sqrt{\delta} \leq 2\sqrt{(\varepsilon^2/4)} \leq \varepsilon$$

then for each $f \in A$ and each $x, y \in [0, 1]$,

$$|f(x) - f(y)| < \varepsilon \text{ whenever } x, y \in [0, 1] \text{ satisfies } |x - y| < \delta.$$

Thus A is an equicontinuous family of functions.

The hypotheses from Thm 3.12 are satisfied and so A is $d_{\max}$ -sequentially compact.

- (b) Define the function $g : [0, 1] \rightarrow \mathbb{R}$, $g(t) = \sin t$.

The sine function is $(d^{(1)}, d^{(1)})$ -continuous on $\mathbb{R}$ (HB p66) and so g is $(d_{[0,1]}^{(1)}, d^{(1)})$ -continuous (Restriction Rule HB p66). Then the product fg is $(d_{[0,1]}^{(1)}, d^{(1)})$ -continuous by the Product Rule (HB p65) and so $fg \in C[0, 1]$.

Then $F(f) = \int_0^1 (fg)(t) dt$ is $(d_{\max}, d^{(1)})$ -continuous on $C[0, 1]$ (HB p79).

Since A is $d_{\max}$ -sequentially compact, and F is $(d_{\max}, d^{(1)})$ -continuous, we can apply the Generalised Extreme Value Theorem (Th 2.13 HB p129).

F is bounded on A and achieves its bounds. In particular, it achieves a minimum on A .

Question 7

- (a) Since $|G| = 44 = 2^2 \times 11$, by Sylow's First Theorem (Th. 1.12, HB, page 39), G has Sylow 2-subgroups of order 4; let m_4 be their number. Then, by Sylow's Second and Third Theorem, we have

$$m_4 \equiv 1 \pmod{2}, \quad m_4 \mid 11 \Rightarrow m_4 = 1 \text{ or } m_4 = 11$$

Hence G has either 1 or 11 Sylow 2-subgroups.

- (b) As in part a), since $|G| = 44 = 2^2 \times 11$, by Sylow's First Theorem (Th. 1.12, HB, page 39), G has Sylow 11-subgroups of order 11; let m_{11} be their number. Then, by Sylow's Second and Third Theorem, we have

$$m_{11} \equiv 1 \pmod{11}, \quad m_{11} \mid 4 \Rightarrow m_{11} = 1$$

Hence G has only one subgroup of order 11.

Since the Sylow 11-subgroup is unique, by Lemma 1.9, page 39, HB, this subgroup (call it K) is normal.

- (c) If G has only one Sylow 2-subgroup (call it H), it follows that this group is normal (Lemma 1.9 again). But then we have that:

1. $|G| = |H| \times |K|$;
2. $|H| = 4$ and $|K| = 11$ are coprime;
3. H and K are normal subgroups of G ;

therefore, by Theorem 2.3, page 39 HB, the group G is the internal direct product of its two Sylow subgroups, i.e. $G = H \times K$.

Now, the only groups of order 4 are the cyclic group $\mathbb{Z}_4$ and the Klein group $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, both Abelian, and the only group of (prime) order 11 is the cyclic group $\mathbb{Z}_{11}$, which is Abelian. Since the direct product of two Abelian groups is Abelian, then G is Abelian.

Proof: given two elements (h_1, k_1) and (h_2, k_2) of $G = H \times K$, we have

$$\begin{aligned} (h_1, k_1)(h_2, k_2) &= (h_1 h_2, k_1 k_2) && \text{(by def. of product)} \\ &= (h_2 h_1, k_2 k_1) && \text{(because H, K are Abelian)} \\ &= (h_2, k_2)(h_1, k_1) \end{aligned}$$

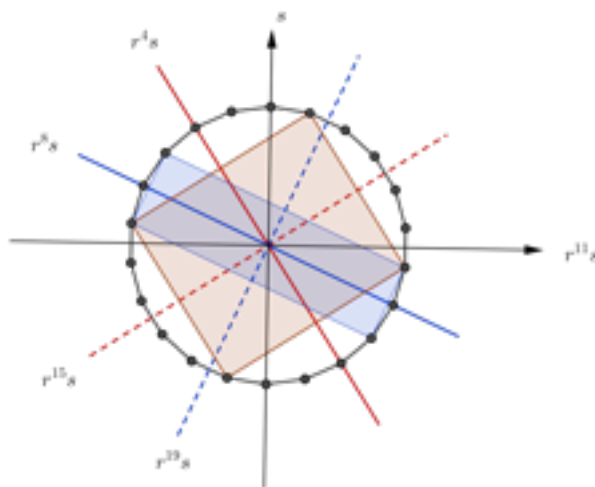
hence $H \times K$ is Abelian (perhaps Theorem 2.2, page 39 HB should also be called, but it does not state clearly the equivalence).

Hence either $G \cong \mathbb{Z}_4 \times \mathbb{Z}_{11}$ or $G \cong V \times \mathbb{Z}_{11}$ (which is equivalent to $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{11}$).

- (d)
- (i) Since D_{22} is a *non-Abelian* group of order 44, by (c) it cannot have a single Sylow 2-subgroup, hence it must have 11 of them (the only other possibility).

- (ii) The dihedral group D_{22} has no element of order 4 (a reflection has order 2; a rotation has order which must be a divisor of 22). Hence, all Sylow 2-subgroups of D_{22} are isomorphic to the Klein group, which contains the identity e , one rotation through π , which necessarily is r^{11} , and two reflections a, b in two perpendicular axes of symmetry (observe that there are exactly 11 axes passing through two vertices and 11 axes perpendicular to them, passing through the midpoints of the sides of the 22-gon).

This can also be seen by remembering that the Klein group is the group of symmetries of a rectangle, and by considering how rectangles with vertices coincident with the vertices of the regular 22-gon can be drawn.



- (iii) It is immediate to spot one of the Sylow 2-subgroups, namely the one containing $s, r^{11}, r^{11}s$, i.e.

$$H_0 = \{e, s, r^{11}, r^{11}s\} = \{r^i s^j : i = 0, 11, j = 0, 1\}$$

Now, every axis through two vertices corresponds to the reflection $r^{2k}s$ and the axis which is perpendicular to corresponds to the reflection $r^{2k+11}s$, so the standard form of the Sylow 2-subgroups of D_{22} is

$$H_k = \{e, r^{11}, r^k s, r^{k+11}s\}$$

for $k = 0, 1, \dots, 10$.

As a Check, here is the Cayley table of these groups:

	e	r^{11}	$r^k s$	$r^{k+11}s$
e	e	r^{11}	$r^k s$	$r^{k+11}s$
r^{11}	r^{11}	e	$r^{k+11}s$	$r^k s$
$r^k s$	$r^k s$	$r^{k+11}s$	e	r^{11}
$r^{k+11}s$	$r^{k+11}s$	$r^k s$	r^{11}	e

Constructing the table would not be expected in an exam.

An alternative argument is to describe H_0 as above and then observe that, by Sylow's Third Theorem (a), all other Sylow 2-subgroups are conjugates of H_0 , i.e.

$$H_k = r^k H_0 r^{-k}, k = 1, 2, \dots, 10$$

Or one could also observe that the subgroups H_k must contain the identity e , r^{11} and a reflection of the form $r^k s$, so by closure the missing element is $r^{11+k} s$.

Question 8

- (a) We begin by assuming that $\{p_1, p_2, \dots, p_n\}$ is the set of all primes of the form $3k + 2$ and we present the positive integer

$$\begin{aligned}
 N &= (p_1 p_2 \dots p_n)^2 + 1 \\
 &= [(3k_1 + 2)(3k_2 + 2) \dots (3k_n + 2)]^2 + 1 \\
 &\equiv (2^n)^2 + 1 && (\text{mod } 3) \\
 &\equiv 2^{2n} + 1 && (\text{mod } 3) \\
 &\equiv 4^n + 1 && (\text{mod } 3) \\
 &\equiv 1^n + 1 && (\text{mod } 3) \\
 &\equiv 2 && (\text{mod } 3)
 \end{aligned}$$

So N is of the form $3k + 2$.

Aiming for a contradiction, we assume that N has no divisors which are congruent 2 modulo 3.

So all the prime divisors of N are congruent 1 modulo 3 (with one congruent 0 modulo 3 if 3 divides N). The product of all these divisors is congruent 1 modulo 3 (or 0 modulo 3 if 3 divides N). But N is congruent 2 modulo 3 so we have our contradiction and N must have at least one prime divisor which is congruent 2 modulo 3.

Now we have that some prime $p = 3n + 2$ divides N and by our assumption that the set $\{p_1, p_2, \dots, p_n\}$ is the set of all primes of this form, p must be in this set.

So $p|N$ and $p|p_1 p_2 \dots p_n$ implies that $p|(p_1 p_2 \dots p_n)^2$ and $p|N - (p_1 p_2 \dots p_n)^2$ which gives us $3n + 2|1$. Which is a contradiction.

So we conclude that there are an infinite number of primes of the form $3k + 2$.

- (b) It is immediately evident that $4 = 2 \times 2$. It remains to be shown that this factorisation is not unique in the ring $\mathbb{Z}[\sqrt{-3}]$.

Using the norm $N(a + b\sqrt{-3}) = a^2 + 3b^2$, $a, b \in \mathbb{Z}$, we see that $N(4) = 16$. As N is the square of the complex modulus, we know that N is multiplicative.

Thus, the norm of any divisor of 4 must be a divisor of 16. This gives us possible values of 2, 4, 8 and 16. So taking each of these in turn we have

$$a^2 + 3b^2 = 2$$

which has no solutions for $a, b \in \mathbb{Z}$.

$$a^2 + 3b^2 = 4$$

has solutions $a = \pm 2, b = 0$ (which we have already established) and $a = \pm 1, b = \pm 1$.

Pausing here we note that $N(4) = N(r)N(s)$ where r and s may be of the form $\pm 1 \pm \sqrt{-3}$. By inspection we find that

$$4 = 2 \times 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

We now show that 2 and $1 \pm \sqrt{-3}$ are irreducible in $\mathbb{Z}[\sqrt{-3}]$.

Suppose $2 = rs$, $r, s \in \mathbb{Z}[\sqrt{-3}]$, neither being a unit. Then

$$N(2) = 4 = N(r)N(s) = 2 \times 2$$

and we have already shown that no member of $\mathbb{Z}[\sqrt{-3}]$ has a norm of 2. So $r, s \notin \mathbb{Z}[\sqrt{-3}]$ and 2 is irreducible in $\mathbb{Z}[\sqrt{-3}]$.

A similar argument shows that $1 \pm \sqrt{-3}$ is also irreducible in $\mathbb{Z}[\sqrt{-3}]$.

Since the units of $\mathbb{Z}[\sqrt{-3}]$ are ± 1 (cf Ch.12, Ex 2.6) it is immediately evident that 2 and $1 \pm \sqrt{-3}$ are not associates and we conclude that $\mathbb{Z}[\sqrt{-3}]$ is not a UFD.

Question 9

- (a) For
- $t \neq 0$
- , we have

$$d((1, 0), (1, t)) = d^{(2)}((1, 0), (0, 0)) + d^{(2)}((1, t), (0, 0)) = 1 + \sqrt{1 + t^2},$$

and

$$d((0, 0), (0, t)) = d^{(2)}((0, 0), (0, 0)) + d^{(2)}((0, t), (0, 0)) = 0 + \sqrt{t^2} = |t|.$$

- (b) The sequence
- $((1, \frac{1}{n}))_{n \in \mathbb{N}}$
- is not convergent; we show this by contradiction. Let us suppose that
- $(1, \frac{1}{n}) \rightarrow (a, b) \in \mathbb{R}^2$
- as
- $n \rightarrow \infty$
- . Now because
- $(1, \frac{1}{n})$
- is not eventually constant, we have

$$d\left((a, b), (1, \frac{1}{n})\right) = d^{(2)}((a, b), (0, 0)) + d^{(2)}((1, \frac{1}{n}), (0, 0)) \geq d^{(2)}((1, \frac{1}{n}), (0, 0)) = \sqrt{1 + \frac{1}{n^2}} > 1$$

for all $n \in \mathbb{N}$. Hence $d((a, b), (1, \frac{1}{n})) \not\rightarrow 0$ as $n \rightarrow \infty$ - a contradiction - and so $((1, \frac{1}{n}))_{n \in \mathbb{N}}$ is not d -convergent.

The sequence $((0, \frac{1}{n}))_{n \in \mathbb{N}}$ converges to $(0, 0)$. We show this as follows: because $(0, \frac{1}{n})$ is not eventually constant, we have

$$d\left((0, 0), (0, \frac{1}{n})\right) = d^{(2)}((0, 0), (0, 0)) + d^{(2)}((0, \frac{1}{n}), (0, 0)) = \frac{1}{n} \rightarrow 0$$

as $n \rightarrow \infty$, and so $((0, \frac{1}{n}))_{n \in \mathbb{N}}$ d -converges to $(0, 0)$.

- (c)

- (i) If the sequence
- (a_n)
- is
- d
- Cauchy then by Definition 1.3 Ch.23, we have that for any
- $\varepsilon > 0$
- , there is an
- $N \in \mathbb{N}$
- such that
- $d(a_m, a_n) < \varepsilon$
- for all
- $m, n > N$
- . Now since
- (a_n)
- is not eventually constant,
- $d(a_m, a_n) = d^{(2)}(a_m, (0, 0)) + d^{(2)}(a_n, (0, 0)) < \varepsilon$
- for all
- $m, n > N$
- .

Now since $\varepsilon > 0$ can be arbitrarily small it is obviously true that $d(a_m, a_n) = d^{(2)}(a_m, (0, 0)) + d^{(2)}(a_n, (0, 0)) < \varepsilon$ implies that $d^{(2)}(a_n, (0, 0)) < \varepsilon$ for all $n > N$. Hence $d^{(2)}(a_n, (0, 0)) \rightarrow 0$ as $n \rightarrow \infty$ and so $(d^{(2)}(a_n, (0, 0)))$ is a null sequence which in turn implies that the limit of the sequence (a_n) is $(0, 0)$.

- (ii) By part (c)(i) we have that each
- d
- Cauchy sequence which is not eventually constant converges to
- $(0, 0)$
- , which is a point in
- $\mathbb{R}^2$
- . Each eventually constant sequence is
- d
- Cauchy since
- $d(a_n, a_m) = 0$
- for all
- $m, n > N$
- , for some
- $N \in \mathbb{N}$
- (by Definition 3.4 Ch. 14). Hence all
- d
- Cauchy sequences converge in
- $\mathbb{R}^2$
- which ensures that
- $(\mathbb{R}^2, d)$
- is a complete metric space by Definition 2.1 Ch.23.

- (d) Let
- $U = \{(x, y) \in \mathbb{R}^2 : y < 0\}$
- . Now since all
- d
- convergent sequences are
- d
- Cauchy, and we know that all
- d
- Cauchy sequences in
- $(\mathbb{R}^2, d)$
- are either eventually constant or convergent to
- $(0, 0)$
- , the closure of
- U
- must be
- $U \cup \{(0, 0)\}$
- .

- (e) Consider the sets
- $U = \{(x, y) \in \mathbb{R}^2 : y < 0\}$
- and
- $V = \{(x, y) \in \mathbb{R}^2 : y \geq 0\} - \{(0, 0)\}$
- . Then we have that
- $\mathbb{R}^2 - (0, 0) = U \cup V$
- , and by part (d),
- $\text{Cl}_{(\mathbb{R}^2, d)}(U) \cap V = \emptyset$
- ,
- $\text{Cl}_{(\mathbb{R}^2, d)}(V) = V \cup (0, 0)$
- and so
- $U \cap \text{Cl}_{(\mathbb{R}^2, d)}(V) = \emptyset$
- .

Hence the two sets U and V satisfy the criteria of Lemma 3.22 Ch.21 and so form a disconnection of $(\mathbb{R}^2 - \{(0, 0)\}, d)$ which is therefore not d -connected.

Later (2019) a discussion emerged which hinged on the fact that in part (e) we should be clear to frame an argument that paid due attention to the induced metric on $\mathbb{R}^2 - \{(0, 0)\}$.

For convenience, we let $X = \mathbb{R}^2 - \{(0, 0)\}$.

A very neat and appealing solution depends on the fact that for every $\mathbf{a} \in X$, the singleton $\{\mathbf{a}\}$ is d -open and so d_X -open and the result follows. (One can prove this by noting that the d -open ball centered at $\mathbf{a} \neq (0, 0)$ with radius $d^{(2)}((\mathbf{a}), (0, 0))/2$ is $\{\mathbf{a}\}$.)

But the other parts of the question seem to be pointing us towards a different answer. So let's explore that.

From part(d) it follows that the set $A \cup \{(0, 0)\}$ is d -closed (being the d -closure of A). It follows that A is d_X -closed. (Intersecting $A \cup \{(0, 0)\}$ with X just removes the point $(0, 0)$.)

Arguing as above in part (d), we can show that $\{(x, y) \in \mathbb{R}^2 : y \geq 0\}$ is also d -closed and so $B = \{(x, y) \in \mathbb{R}^2 : y \geq 0\} - \{(0, 0)\}$ is d_X -closed.

Clearly, A, B are non-empty and $A \cup B = X$ Thus $\{A, B\}$ is a d_X -disconnection of X showing that X is not d_X -connected.